CONTACT:
Research Section
5000 NASA Blvd., Suite 2400
Fairmont, WV 26554
Ph: 877-628-7674
Fax: 304-366-9095
Web: www.nw3c.org

Criminal Use of Social Media (2013)

Defining social media is difficult because it is ever changing like technology itself, but for the purposes of this paper, social media will be defined as any website or software that allows you to receive and disseminate information interactively.

The tremendous rise in popularity of social media over the past seven years has led to a drastic change in personal communication, both online and off. Comparing to the world population clock, the total world population is around 7.06 billion.[1] With that being said, the popularity of sites such as Facebook, (1.06 billion monthly active users)[2], YouTube (800 million users)[3], Twitter (500 million users)[4], Craigslist (60 million U.S. users each month)[5], and Foursquare (has a community of over 30 million people worldwide)[6] has connected people from all over the world to each other, making it easier to keep in touch with friends, loved ones, or find that special someone. In addition to personal usage, businesses and the public sector use social media to advertise, recruit new employees, offer better customer service, and maintain partnerships.[7] In fact, 65% of adults now use social media.[8] Social networking is the most popular online activity, accounting for 20% of time spent on PCs and 30% of mobile time.[9] As social interactions move more and more online, so does the crime that follows it.

Crimes Linked to Social Media

Social networking consists of websites that allow users to create an online profile in which they post up to the minute personal and professional information about their life that can include pictures, videos, status updates, and related content. Social networking is a potential gold mine for criminals who leverage the users' personal details into financial opportunity.

Burglary via Social Networking

The classic example of exploitation on social networking sites involves the perpetrator perusing users' profiles and looking for potential victims in the vicinity who won't be home. Myspace and Facebook users can post that they will be out for the evening, which gives potential thieves a large time window to burgle the property. Facebook and Twitter now have a new "my location" feature allowing readers to see where they were and how long ago it was when they posted their update, making it that much easier for criminals to attack.[10] (See Cybercasing Section Below) Stories of this nature are frequently in the media[11] and serve as a reminder that users are not as cautious as they should be with their personal information. The thieves see a status update of a family being on vacation for an extended period of time and jump at the perfect opportunity to steal some valuables.[12] Another example of a recent investigation in New Hampshire ended when thieves who used Facebook to profile victims, were caught using a very peculiar type of firework that was recently taken in a burglary. An off-duty officer investigated firework explosions he could hear in the distance. The fireworks were stolen in the series of break-ins over the prior month.[13]

Some other social networking applications, such as Foursquare and Gowalla are primarily location-based networks. Users of these networks can be rewarded for posting their locations frequently and are then given temporary titles while at their location--for example, posting that you're having a cup of coffee at Starbucks may make you the Mayor of Starbucks on this certain site.[14] As previously mentioned, posting a location allows perpetrators the perfect window to commit a burglary, vandalism, or even a home invasion.

Phishing & Social Engineering

A variety of forms of identity theft are performed daily on social networking sites under the guise of other tasks. For example, one technique is called phishing, which involves making attempts to acquire passwords, account numbers, and related information. It is said that phishing has become the most widespread Internet and email scam today.[15] The term is a play on the actual sport of "fishing," in which perpetrators send out many (sometimes millions) of emails with the hopes of getting "bites" in return. Despite the low success rate, criminals continue to send out emails that look like legitimate concerns over account security or sale reminders from your favorite retailer.[16] Beware of the requests to discontinue emails that you believe are scam, this is a way that phishers can tell if an email is still active or not. Phishers can take this request to discontinue, note that the address is a true email address, and send more scams from a new account. In 2012, there were nearly 33,000 phishing attacks globally each month which totaled a loss of $687 million. These phishing attacks mark a 19% increase globally compared to the first half of 2011.[17]

Another technique of crime on social networking sites is social engineering. In a classical sense, social engineering refers to the social manipulation of large groups of people to meet political or economic ends. Today, it has taken on an additional meaning in the cyber security world.

Social engineering refers to gaining access to information by exploiting human psychology rather than using traditional hacking techniques.[18] A classic example of this starts with a friend on your network sending you a message asking for a quick loan to get car repairs so he/she can get home for work on Monday, and ends with you finding out a few days later that your friend never needed car repairs and that the person you transferred money to was a scam artist. This form of social engineering is surprisingly easy to achieve, and because of it, the computer **security firm Trend Micro calls Facebook a "minefield of scams."**[19]

All that is needed by the scammer is the username and password of one member of a network and a little practice in writing letters that sound urgent to inspire friends to aid you. All the while the scammer is vague enough not to reveal the impersonation. Even if only a few friends on the list are duped, the return on investment for the scammer is quite high. Social engineering isn't limited to social networking. A recent case involved the software company Oracle. During a convention, a contest was held to demonstrate the dangers of social engineering. Several hackers posed as IT professionals and asked company employees to hand over data and visit websites as part of "routine IT protocol." Oracle employees as well as many others were frighteningly compliant in the demonstration.[20]

Malware

Last, social networking offers opportunities for virus and malware users. Users clicking on links, opening attachments, and responding to messages on networks can become victims without knowing it, resulting in adware, viruses, and malware being loaded onto their machines. Malware attacks have increased and are only growing because of the use of social media. According to one report, 52% of organizations have experienced an increase in malware attacks as a result of their employees' use of social media.[21] Additionally, the business world is concerned that their employees' online behavior could be putting their network security at risk. Sophos' 2010 Security Report surveyed over 500 organizations and found that 72% were concerned that social networking endangered their security.[22] A 2011 survey done by Socialware found that 84% of financial advisors said they use social networks for business purposes, up from 60% in 2010.[23]

While there is very little risk of contracting malware from Facebook itself (or any other reputable social media site), there are various tricks that scammers can use to get you to leave the protective social media environment without even realizing it. A user must first be tricked into leaving the Facebook world by clicking a link on Facebook that leads to an external website, then a malware attack is able to take place.[24] One technique criminals use to trick users into installing malware is by creating fake pop-ups that look like update screens used by various common web browser plug-ins (such as Adobe Flashplayer), in hopes that users will be used to occasionally updating their software for websites and click on it without a thought.[25] The Sophos' Security Threat Report of 2013 states that in 2012, more than 80% of threats were from redirects, mostly from legitimate sites that had been hacked.[26]

Cybercasing the Joint

Another development in social media technologies is called geotagging, which embeds geographical data (longitude and latitude) into media such as photos, videos, and text messages.[27] Geotagging allows users' locations to be posted along with their media. The location of users can be found quickly and precisely by combining the geotagging of media-friendly sites, such as YouTube, Flickr, Google Maps, Twitter, Facebook, and Craigslist, with all the aforementioned networking sites to triangulate all positions known.[28] Facebook snuck in the "add location" option without letting users know. This feature tacks on information about where the user was and when they were there when they updated their status. For example, at the end of a status it will say "near Cheat Lake approximately 2 minutes ago."[29] This same feature has been added to Twitter, only before composing a tweet it asks whether or not you would like to add your location,[30] a tad more considerate than Facebook, but dangerous nevertheless.

A recent study from the International Computer Science Institute tested the potential to use all publicly available resources to determine the locations of a variety of people on the Internet.[31] A process called cybercasing allows users to access online tools to check out details, make inferences from related data, and speculate about real world locations for questionable purposes. Cybercasers use the Internet to determine the location of a desired victim by accessing any available resource. The cybercasing study used three different websites in their scenarios:

1. The first scenario used the virtual flea market site Craigslist to spot desirable photographs with geotagged data. In most cases, the researchers were able to cross-reference Google Street View to determine the exact address of the poster. Researchers also determined what times were best to burgle a residence by a poster's ad that would often state "Please call after 5 p.m.," implying that they would be gone at work on most days.
2. The second scenario examined the Twitter feed of a well-known reality show host. By viewing the pictures posted on TwitPic with the Firefox plug-in Exif-Viewer, the researchers only had to right click on the celebrity's pictures to reveal geographical coordinates. By taking the average of several pictures posted in a similar region, the researchers could determine the location of the user with great precision.
3. Lastly, YouTube was used to find the home address of someone currently on vacation. By creating a script that collects usernames and downloads the related videos, researchers were able to find a user that lived in the predetermined area of Berkley, CA, and was currently on vacation in the Caribbean, as determined by his most recent YouTube uploads. The researchers were able to use his real name in a Google search to determine his address. The entire process took less than 15 minutes.[32]

Costs and Statistics

The prevalence of criminal activity on social media sites is difficult to determine. In fact, there are currently no comprehensive statistics on social media crimes, although steps are being taken. This can be due to a number of factors, especially considering the broad nature of social media, anonymity afforded to criminals, and relative lack of awareness of Internet users, which can create a ripe environment for victimization. However, we can look into related crimes that can involve social media to estimate how often these crimes occur.

Identity Theft

- The 2011 Internet Crime Report from the Internet Crime Complaint Center (IC3) reported that identity theft was the second highest complaint in 2011. Of the top five reported crime types, Identity theft accounted for almost 22% of complaints.[33]

- The Consumer Sentinel, a database maintained by the Federal Trade Commission (FTC) that collects information about consumer fraud from the FTC and other reporting agencies, reported that the number one complaint category was identity theft with 279,156 complaints (15% of all complaints) received by the Consumer Sentinel in 2011.[34]

- The identity theft survey released in 2012 by Javelin Strategy and Research revealed that identity fraud had increased by 13% in 2011, suggesting that 11.6 million Americans were ID theft victims in 2011. Despite this increase, the amount stolen remained steady. The mean costs to resolve the crime was $631, which was the highest average dollar amount since 2007.[35]

Cyberstalking

- Stalking usually refers to harassment or threatening behavior that an individual engages in repeatedly. Results from the 2010 National Intimate Partner and Sexual Violence Survey show that 1 in 6 women (16.2%) and 1 in 19 men (5.2%) in the United States have experienced stalking at some point during their lifetime. Most victims of stalking are under the age of 25. According to the Centers for Disease Control and Prevention, more than half of female victims and more than one-third male victims of stalking say it happened before the age of 25. About 1 in 5 females and 1 in 14 male victims experience stalking between the ages of 11 and 17. Receiving unwanted phone calls, voicemails, and text messages is the most common experienced stalking tactic for both male and female victims. [36]

- In 2011, statistics of cyberstalking victimization compiled by Who@ showed that harassment most often originated through emails, comprising 32% of cases followed by Facebook with 16%. Of all cases reported, 80% escalated in some way. The top three ways in which incidents escalated were through online phone calls (27%), email (16%) and Facebook (11.5%).[37]

- Cyberstalking is becoming more common than physical harassment. Men are more likely to be targeted by strangers than women. Around 37% of men, and 23% of women were said to be

stalked by complete strangers. Most victims of these stranger attacks do not know where they came from. 1 in 5 said the offender targeted them via social networking sites and 16% from blogging forums.[38]

The statistics reviewed suggest that identity theft and stalking/cyberstalking are prevalent and costly crimes. In addition, social media such as Facebook, Twitter, YouTube, and Flickr all offer an avenue of contact for potential perpetrators. Currently, there is no way to determine the overall occurrence of crimes on social media, but the preceding suggests that social media sites are ideal outlets for fraudsters and stalkers.

Examples/Case Studies

- A fake Facebook "security team" will send users messages about the suspension of their page because they are in violation of the Terms of Service. The message will state that if you believe this is a mistake, you can click on the link provided to verify your account. Users may believe this is a legitimate message from Facebook; therefore they click the link in order to not lose their Facebook. Doing this they are giving the faulty site their user information. This message is an example of a scam because it seeks to harvest your log-in credentials. The link is apps.facebook.com/PageSecurityTeam/. Scammers will use official sounding page names to make their schemes seem legitimate to users. Their end result is may be to obtain your user name and password.[39]

- In 2007, the dangers of cyberbullying were brought to light when a teenage girl, Megan Meier, committed suicide when it was revealed that a boy she admired on Myspace was actually a classmate's mother antagonizing the teenager for being different.[40] The mother, Lori Drew, allegedly communicated to Megan as "Josh" for over one month and then abruptly ended the relationship. Megan committed suicide the same day. Lori Drew was convicted of computer fraud and abuse, but was acquitted for Meier's death.[41] A more recent event of cyberbullying happened on the campus of Rutgers University where a boy, Tyler Clementi, was videotaped by his roommate kissing another male and put on the campus' live stream for everyone to watch. The status of Clementi's sexual orientation was unknown at the time. Clementi was so mortified from the stream that he committed suicide by jumping off of the George Washington Bridge.[42]

- In 2009, Justin Brown was arrested for impersonating a model named Bree Condon on the dating site Seekingmillionaire.com. Unlike many scams perpetrated on social networking sites, Mr. Brown impersonated a real model and assumed her real name. Ms. Condon hired a private investigator who ultimately alerted police to the fraud that her name, likeness, and professional photographs were being used in the scam until Mr. Brown was arrested. Investigators later learned that Mr. Brown had phone conversations with wealthy men in exchange for money and gifts (iPhone and $15,000 cash). The scam is an exception considering the care that Mr. Brown took and demonstrates what can be perpetrated by a lone individual. Mr. Brown said that he created a plausible biography of Ms. Condon by using her online biographical information. While the following did not occur on a social media site discussed yet in this paper, the exact scenario could happen on any social networking site.[43] The recent MTV tv series Catfish displays this impersonation and lying through internet sites. Often times on the show, each party has only communicated via text, chat, email, and sometimes phone calls. Very rarely does the "couple" meet in person to see if who they think they are talking to is the real deal. The show displays how easily it is to become someone else online and trick others into falling for this false person. The

show Catfish takes viewers on the journey to see if the person on the other end of the keyboard is who they say they are.[44]

- In 2013, Two teenagers on the Steubenville Ohio football team were found guilty of the rape of a 16 year old girl. Although the victim could not recall most of the details of her assault, the boys were convicted based predominantly on text messages and shared cell phone photos taken during the assault that they shared on social media. [45]

The IACP Center for Social Media

In 2010, the Department of Justice authorized a new initiative to assist law enforcement to increase awareness of recent developments of social media in the Web 2.0 era. The International Association of Chiefs of Police (IACP) operate the Center for Social Media; the goal of which is to enhance law enforcement's ability to use social media to solve crimes, strengthen police-community relations, and enhance services.

The IACP Center for Social Media provides a variety of information from the basics of social media technologies available to law enforcement, case studies, an active directory of law enforcement agency social media sites, and a current blog full of recent information.

If you are interested in providing social media awareness for your agency, visit www.iacpsocialmedia.org and click on the "Getting Started" tab.

"For More Information" Links

- Internet Crime Complaint Center – http://www.ic3.org
- International Associate of Chiefs of Police Social Media Project – http://www.iacpsocialmeda.org
- Privacy Rights Clearinghouse – http://www.privacyrights.org/
- Please Rob Me (Dangers of Over Sharing) – http://www.pleaserobme.com

Primary Author: Jason Boone, NW3C Research Associate
Updated 2013 By: Stephenie Nagy, NW3C Research Intern